UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/027,622	12/19/2001	Kenneth W. Aull	NG(MS)7194	2941

26294 7590 08/08/2008

TAROLLI, SUNDHEIM, COVELL & TUMMINO L.L.P.
1300 EAST NINTH STREET, SUITE 1700
CLEVEVLAND, OH 44114

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2137	
MAIL DATE	DELIVERY MODE
08/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte KENNETH W. AULL, THOMAS C. KERR,
WILLIAM E. FREEMAN, and MARK A. BELLMORE

Appeal 2008-1980
Application 10/027,622
Technology Center 2100

Decided: August 7, 2008

Before JEAN R. HOMERE, JAY P. LUCAS, and STEPHEN C. SIU, *Administrative Patent Judges*.

SIU, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1-16. We have jurisdiction under 35 U.S.C. § 6(b). We reverse.

A. INVENTION

The invention at issue involves generating certificates and private keys wrapped in a public key (Spec. 7). In particular, a token ID and user signature certificate is read from a token and matched to data in a database. A certificate/private key is created and wrapped with a public key associated with the token ID. The certificate/private key is downloaded to the token (*id.* 7) such that data transmitted between the token and a client platform is secure (*id.* 12).

B. ILLUSTRATIVE CLAIM

Claim 1, which further illustrates the invention, follows:

1. A method for assigning certificates and associated private keys to a token, comprising:

accessing the token through a token reader connected to a computer system by a certificate authority;

reading a token ID and a user signature certificate from the token;

searching for a match for the token ID and the user signature certificate in an authoritative database;

creating a certificate and an associated private key, wherein the certificate and the associated private key are wrapped with a public key associated with the token ID and digitally signing the certificate and the associated private key using a signature certificate of the certificate authority if a match for the token ID and the user signature certificate is found in the authoritative database;

downloading the certificate and the associated private key to the token; and

decrypting the certificate and the associated private key using a private key stored in the token, such that the token stores at least the token ID, the private key, the user signature certificate and the certificate and the associated private key.

C. REJECTION

Claims 1-6, 8-14, and 16 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,192,131 ("Geer") and U.S. Patent No. 6,615,171 ("Kanevsky"). Claims 7 and 15 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Geer, Kanevsky, and U.S. Patent Publication No. 2003/0005291 ("Burn").[1]

II. ANALYSIS

Claim 1 and claim 9 recite accessing a token by a certificate authority, creating a certificate and an associated private key, and downloading the certificate and the associated private key to the token.

Appellants assert that "Geer does not teach or suggest that the disclosed certifying authority 18 can access a token" (App. Br. 9) and that "Geer taken in view of Kanevsky does not teach or suggest downloading a certificate and an associated private key to [the] token" (App. Br. 10).

---

[1] Claim 8 depends from claim 7 and therefore recites all limitations of claim 7. Similarly, claim 16 depends from claim 15 and recites all limitations of claim 15. We therefore, consider the Examiner's rejection of claim 8 and claim 16 under the rejection under 35 U.S.C. § 103(a) over Geer, Kanevsky and Burn.

The Examiner finds that Geer discloses a certifying authority accessing a token because "Geer teaches that a certifying authority is necessary to certify the identity of the user . . . [and that] . . . in order to perform the operations . . . the certificate authority must have access to the user's information via the smart card" (Ans. 8). However, the Examiner does not show that Geer also discloses creating a certificate and an associated private key and downloading the certificate and the associated private key to the token, as recited in claim 1 and claim 9. The Examiner states that Geer discloses at col. 9, ll. 24-29 different parties to a business deal in which "***each of the actual parties*** . . . ***obtains*** . . . ***an authorization certificate and a private key of a new public key pair***" and that "each of the parties . . . [in a business deal] . . . use(s) a smart card for maintaining the certificate and private key sent as also mentioned in col. 12, lines 30-37" (Ans. 9).

Geer discloses that parties participating in a business deal obtain "an authorization certificate and a private key" from a "certifying authority computer" (col. 9, ll. 24-29). However, the Examiner has not shown that Geer also discloses that the "certifying authority computer" or any other component reads a token ID and user signature certificate from the token, creates and wraps a certificate and an associated private key with a key associated with the token ID, and downloads the certificate and associated private key to the token.

Similarly, the Examiner does not allege, let alone show, that the addition of Kanevsky or Burn cures the aforementioned deficiency of Geer. Therefore, we reverse the rejection of claims 1 and 9, and of claims 2-8 and 10-16, which depend therefrom.

VI. ORDER

In summary, the rejections of claims 1-16 under 35 U.S.C. § 103(a) are reversed.

REVERSED

Homere, *Administrative Patent Judge, dissenting.*

I write separately to voice my disagreement with the majority's holding that the *Examiner has not shown* that the combination of Geer and Kanevsky renders independent claims 1 and 9 unpatentable. Particularly, the majority finds that the *Examiner has not shown* that the cited combination teaches the limitation of creating a certificate and an associated private key, which are downloaded to a token. Because of this finding, the majority reverses the Examiner's prior art rejection of claims 1 through 16. From that decision, I respectfully dissent.

The majority opinion states in relevant part:

> [T]he *Examiner does not show* that Geer also discloses creating a certificate and an associated private key and downloading the certificate and the associated private key to the token, as recited in claim 1 and claim 9… However, the *Examiner has not shown* that Geer also discloses that the "certifying authority computer" or any other component reads a token ID and user signature certificate from the token, creates and wraps a certificate and an associated private key with a key associated with the token ID, and downloads the certificate and associated private key to the token. (Emphasis added.)

At the outset, I would like to highlight my disagreement with the majority's finding that the *Examiner has not shown* that the combination of Geer and Kanevsky teaches the cited limitations. Our reviewing Court has held that Appellants have the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86

(Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)). In the present appeal to be Board, the Examiner's rejection has addressed the all the limitations of independent claims 1 and 9. (Ans. 3-4.) Further, the Examiner has discussed in great substance her rationale for concluding that the combination of Geer and Kanevsky renders independent claims 1 and 9 unpatentable. (Ans. 7-14.) In my view, the Examiner has adequately established her *prima facie* case of obviousness. Therefore, consistently with these precedents, I would place the burden on Appellants to show that the Examiner has erred in reaching the cited conclusion.

Inconsistently with the cited precedents, however, the majority's holding's appears to be premised upon arguments that Appellants have not even raised in their Briefs. Rather, the majority has chosen to *sua sponte* find that the *Examiner has not shown* that the cited combination teaches creating a certificate and an associated private key. While the majority appears to acknowledge such teaching in Geer, it went on to assert that the *Examiner has not shown* that Geer teaches (1) reading a token ID and a signature certificate from the token, (2) wrapping the certificate and an associated private key, and (3) subsequently downloading them to the token. In my view, such arguments should have been deemed waived since

Appellants failed to raise them. Further, even if Appellants had raised these arguments in a timely manner, I would still agree with the Examiner. As the Examiner correctly pointed out, Geer discloses a certifying authority computer from which each party to a business deal obtains an authorization certificate and a private key that the certifying authority minted using a public key pair minted. (Ans. 3.) One of ordinary skill in the art would readily recognize that by using the public key pair to mint the private key and the authorization certificate, Geer teaches creating a certificate along with an associated private key wrapped with the public key pair. As the Examiner correctly pointed out in the Answer, the ordinarily skilled artisan would aptly appreciate that Geer's certifying authority, in order to perform its conventional certifying functions, it must access and read the user's information in the token (smart card.) (Ans. 8.) I further agree with the Examiner that the ordinarily skilled artisan would readily recognize that by using the public key pair to mint the authorization certificate and associated private key, Geer teaches wrapping said certificate and private key with the public key pair. Additionally, I agree with the Examiner that the ordinarily skilled artisan would aptly appreciate that the certifying authority computer, by sending the created authorization certificate and associated private key to the smart card, teaches downloading said certificate and said private key to the smart card. (Ans. 9.)

I am therefore satisfied that Appellants have not shown that the Examiner erred in finding that the combination of Geer and Kanevsky

renders independent claims 1 and 9. Thus, I cannot agree with the majority's reversal of the Examiner's rejection of the cited claims. Accordingly, I would affirm the Examiner's prior art rejection of independent claims 1 and 9 as being unpatentable over the combination of Geer and Kanevsky.

rwk

TAROLLI, SUNDHEIM, COVELL & TUMMINO L.L.P.
1300 EAST NINTH STREET, SUITE 1700
CLEVELAND, OH 44114